US 20060212936A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2006/0212936 A1**

(43) **Pub. Date: Sep. 21, 2006**

Berzanskis et al.

(54) **METHOD OF INTEGRATING QKD WITH IPSEC**

(76) Inventors: **Audrius Berzanskis**, Cambridge, MA (US); **Harri Hakkarainen**, Los Gatos, CA (US); **Keun Lee**, Newburyport, MA (US); **Muhammad Raghib Hussain**, Pleasanton, CA (US)

Correspondence Address:
MAGIQ TECHNOLOGIES, INC
171 MADISON AVENUE, SUITE 1300
NEW YORK, NY 10016-5110 (US)

(21) Appl. No.: **11/082,068**

(22) Filed: **Mar. 16, 2005**

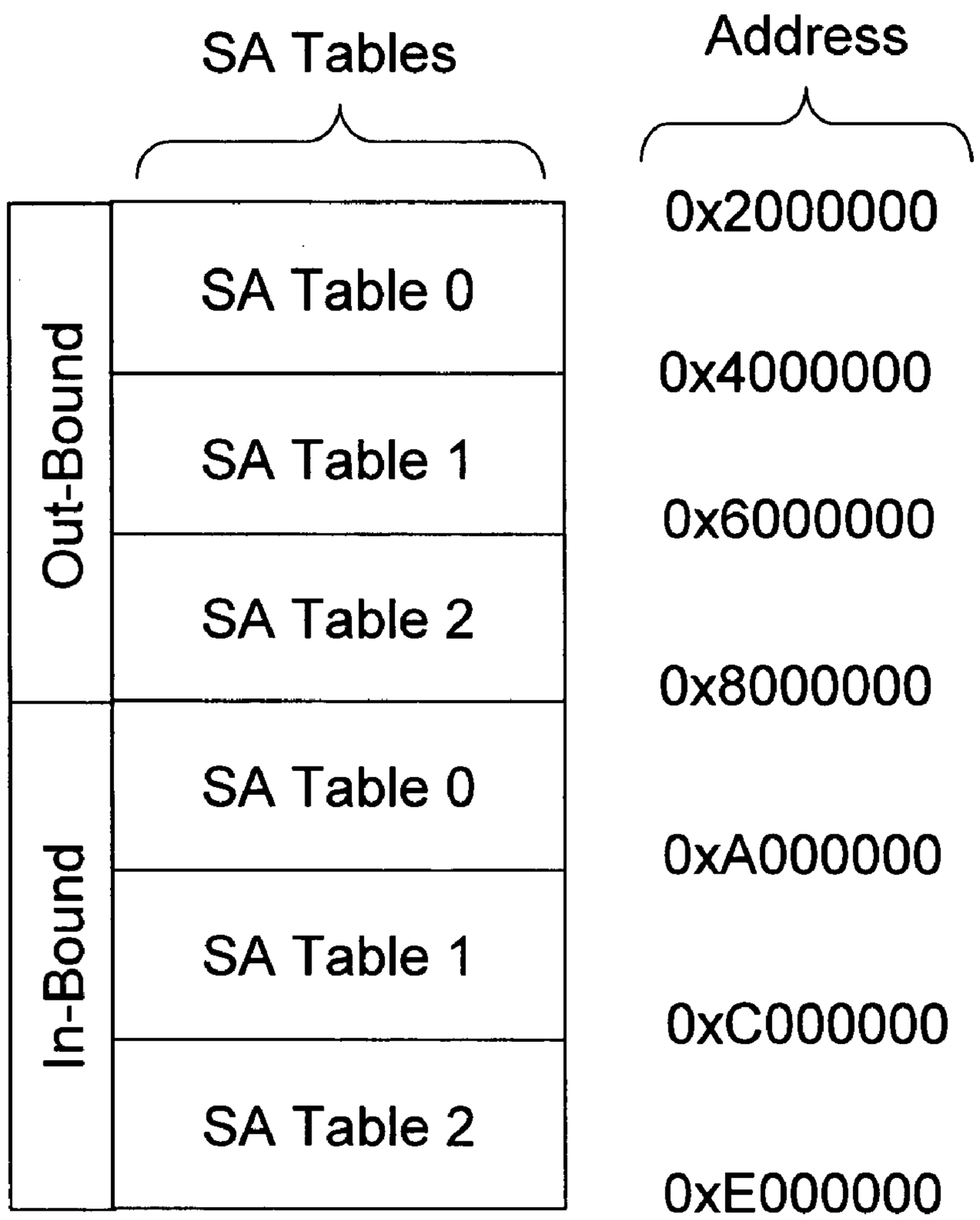
Publication Classification

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **726/14**

(57) **ABSTRACT**

A method of integrating quantum key distribution (QKD) with Internet protocol security (IPSec) to improve the security of IPSec. Standard IPSec protocols impose limits on the frequency at which keys can be changed. This makes efforts to improve the security of IPSec by employing quantum keys problematic. The method includes increasing the size of the Security Association (SA) Table in a manner that enables a high key change rate so that the quantum keys can be combined with the classical keys generated by Internet Key Exchange (IKE). The invention includes a method of creating the SA Table by combining quantum keys generated by the QKD process with classical keys generated by the IKE process, thereby enabling QKD-based IPSec.



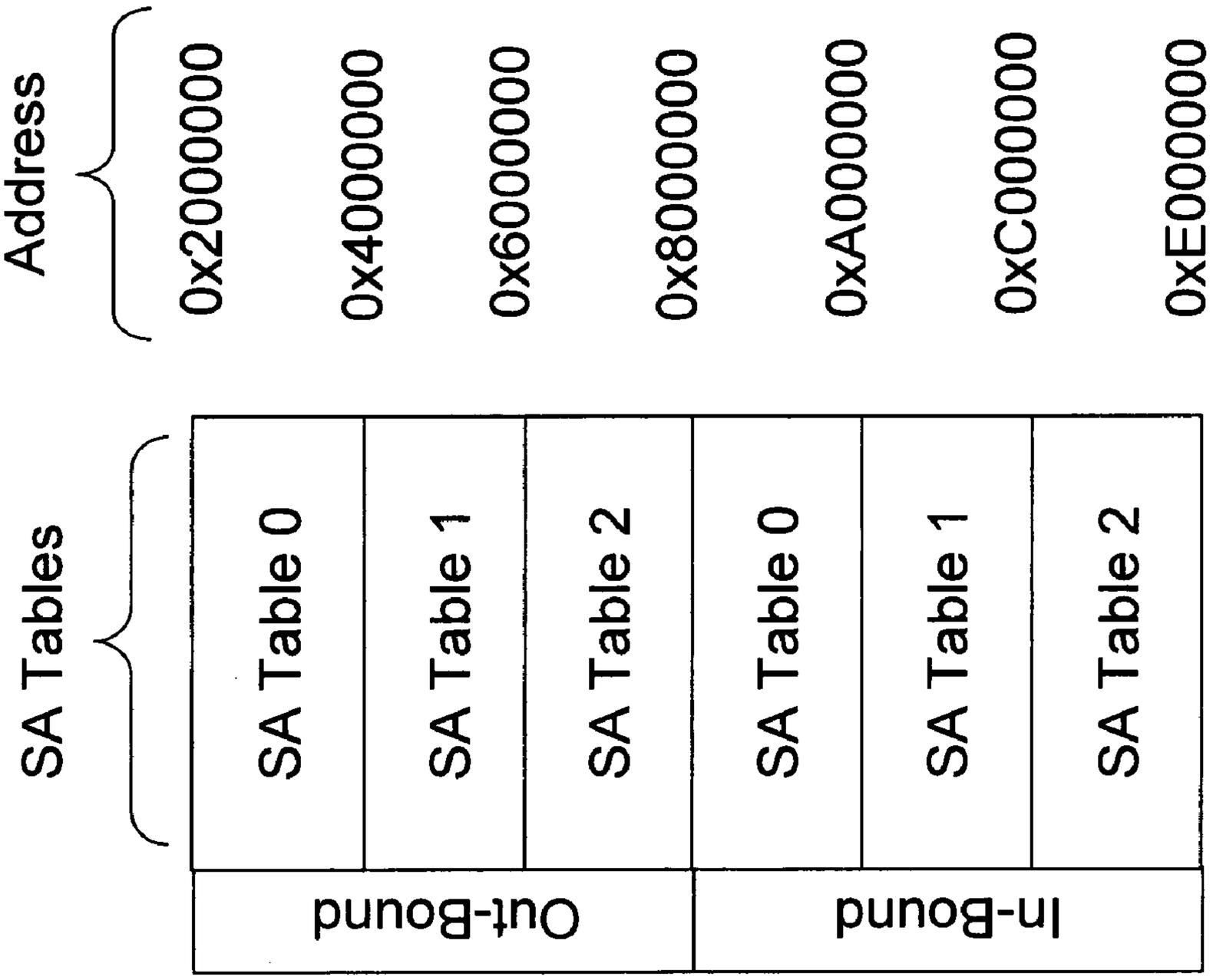

Address
0x2000000
0x4000000
0x6000000
0x8000000
0xA000000
0xC000000
0xE000000
SA Tables
SA Table 0
SA Table 1
SA Table 2
SA Table 0
SA Table 1
SA Table 2
Out-Bound
In-Bound

FIG. 1

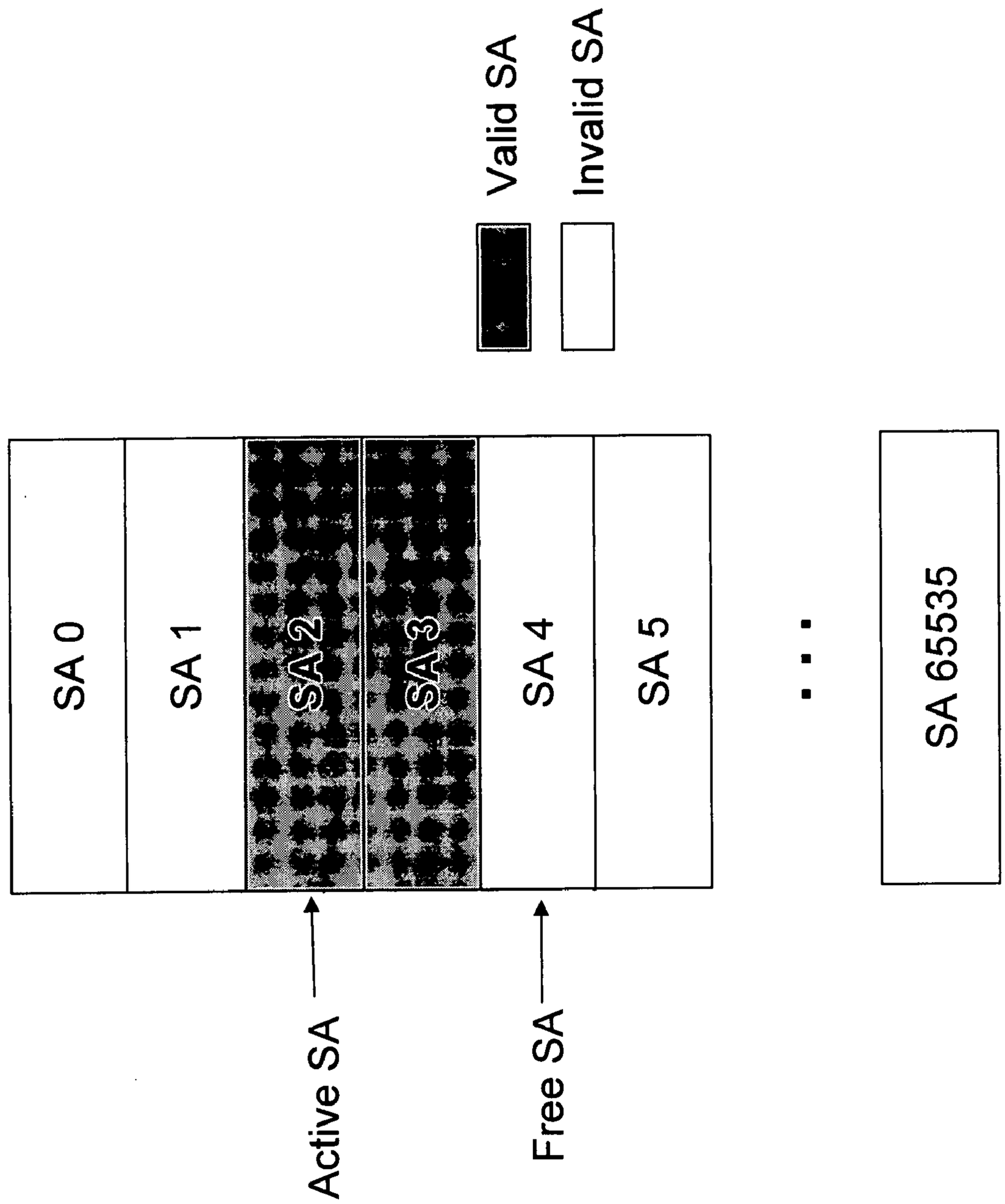
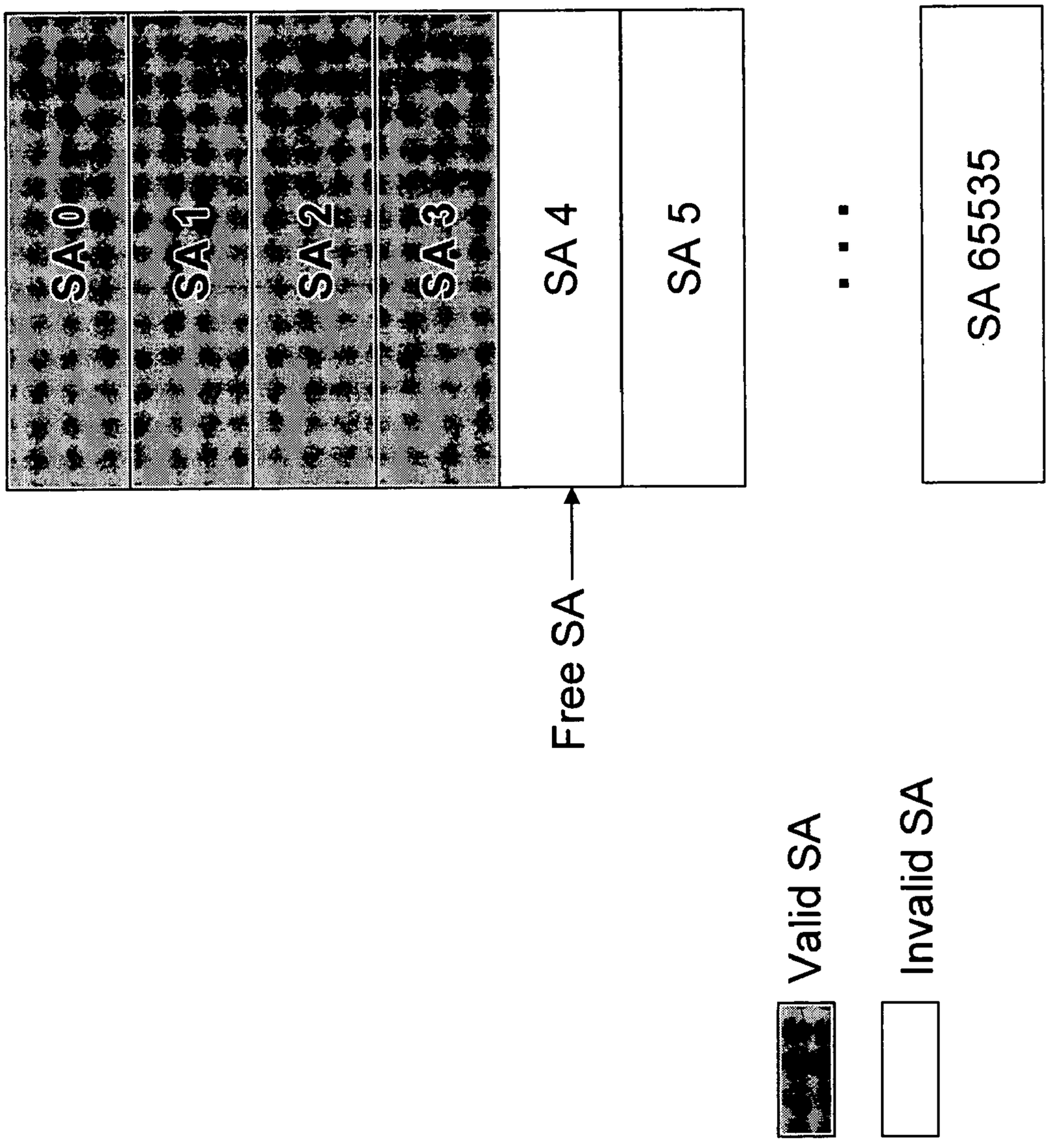

Valid SA
Invalid SA
SA 0
SA 1
SA 2
SA 3
SA 4
SA 5
SA 65535
Active SA
Free SA

FIG. 2

FIG. 3



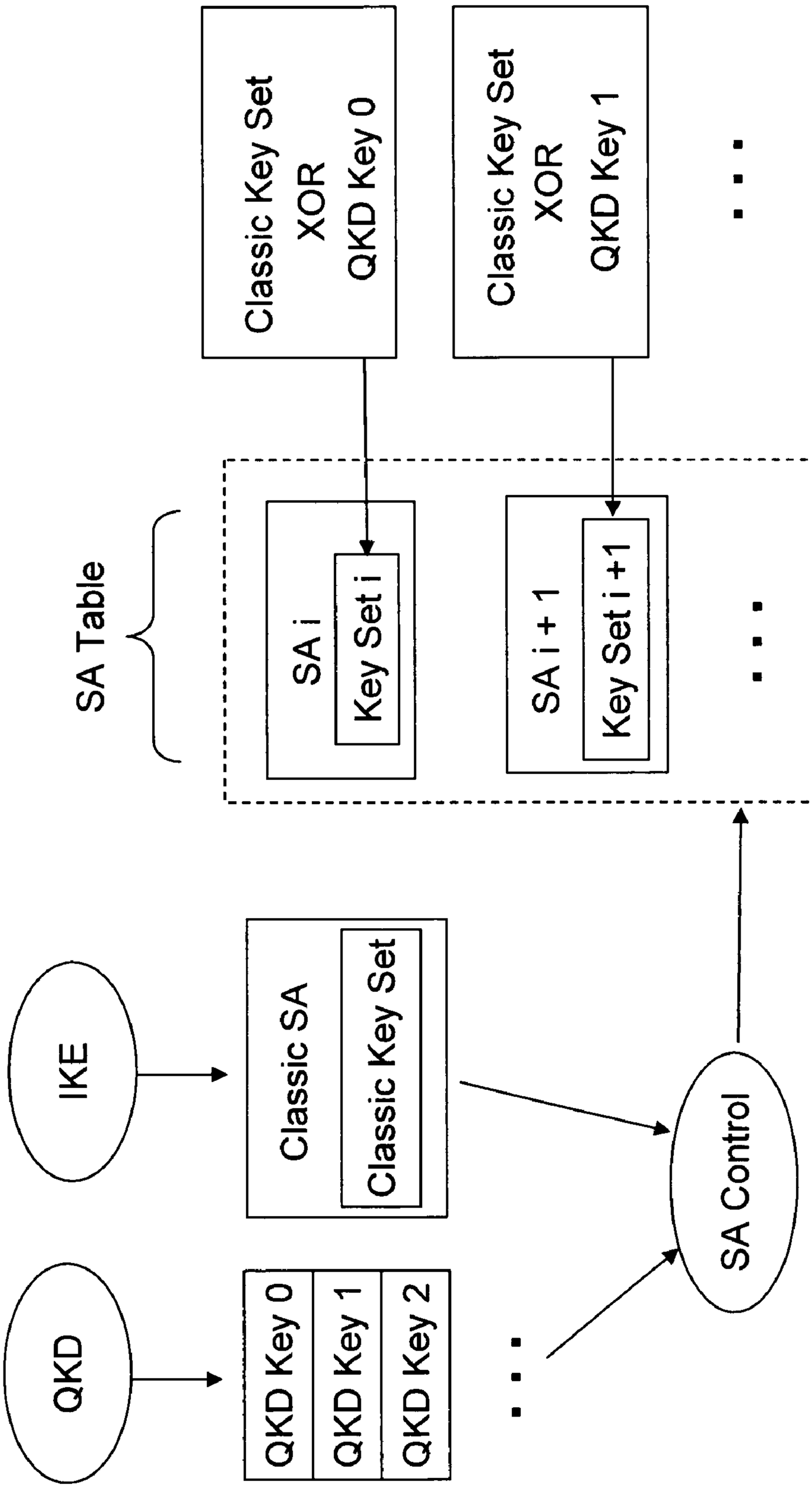

Classic Key Set
XOR
QKD Key 0
Classic Key Set
XOR
QKD Key 1
SA Table
SA i
Key Set i
SA i + 1
Key Set i +1
IKE
Classic SA
Classic Key Set
QKD
QKD Key 0
QKD Key 1
QKD Key 2
SA Control

FIG. 4

METHOD OF INTEGRATING QKD WITH IPSEC

FIELD OF THE INVENTION

[0001] The present invention relates to quantum cryptography and Internet communication, an in particular relates to methods of integrating quantum key distribution (QKD) with Internet protocol security ("IPSec") to provide for enhanced security of Internet-based data communication.

BACKGROUND INFORMATION

Quantum Key Distribution

[0002] Quantum key distribution (QKD) involves establishing a key between a sender ("Alice") and a receiver ("Bob") by sending "qubits" (i.e., weak optical pulses having less than one photon, on average) over a "quantum channel." The security of the key distribution is based on the quantum mechanical principle that any measurement of a quantum system in unknown state will modify its state. As a consequence, an eavesdropper ("Eve") that attempts to intercept or otherwise measure the qubits will introduce errors and reveal her presence. Once a key is successfully established between Bob and Alice, they can communicate over a public channel by using the exchanged key to encrypt their messages using perfectly secure one-time pad encryption or some other symmetric key encryption algorithm. In present-day QKD technology, keys of a suitable length (e.g., 256 bits) can be generated at a rate of about 1-100 per second, depending on the separation between Alice and Bob (e.g., the length of the optical fiber length connecting the two).

[0003] The general principles of quantum cryptography were first set forth by Bennett and Brassard in their article "Quantum Cryptography: Public key distribution and coin tossing," Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984). Specific QKD systems are described in U.S. Pat. No. 5,307,410 to Bennett, which is incorporated herein by reference, and in the article by C. H. Bennett entitled "Quantum Cryptography Using Any Two Non-Orthogonal States", Phys. Rev. Lett. 68 3121 (1992), which is also incorporated herein by reference. The general process for performing QKD is described in the book by Bouwmeester et al., "The Physics of Quantum Information," Springer-Verlag 2001, in Section 2.3, pages 27-33, which is incorporated by reference herein as background information.

IPSec

[0004] The acronym "IPSec" is a contraction of the phase "Internet Protocol (IP) Security." IPSec is a set of protocols developed by the Internet Engineering Task Force (IETF), the main Internet standards organization. The protocols are designed to support the secure exchange of information over the Internet-more specifically, the exchange of packets at the IP layer. IPSec is the most popular method of implementing secure data communication channels over the Internet, and is used widely to provide security for the operation of virtual private networks (VPNs).

[0005] The basics of IPSec are described in the publication by Stephen Kent and Randall Atkinson, entitled, "Security architecture for the Internet Protocol," RFC 2401, published by The Internet Society, 1998, and found at: http://www-.faqs.org/rfcs/rfc2401.html, which publication is incorporated by reference herein.

[0006] When sending information over the Internet, the information is broken up into "packets," which allows for efficient management of Internet traffic. The packets travel separately over the Internet towards a receiving device at a designated address. The packets are then reassembled so that they have their original order at the receiver.

[0007] Sensitive information sent over the Internet can be encrypted via IPSec to maintain the secrecy of the information. IPsec supports "Transport" and "Tunnel" encryption modes. The Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The Tunnel mode encrypts both the header and the payload and is thus more secure. On the receiving side, an IPSec-compliant device decrypts each packet according to the particular encryption mode.

[0008] There are two main IPSec protocols—Authentication Header (AH) and Encapsulating Security Payload (ESP). The AH protocol is mainly used for data authentication purposes, while the ESP protocol provides authentication and data confidentiality. The AH and ESP protocols can protect either an entire IP payload (Tunnel mode) or the upper-layer protocols of an IP payload (Transport mode).

[0009] The operation of IPsec requires the transmitter and receiver in the network to share a set of secret keys. This is accomplished through a protocol known as the "Internet Security Association and Key Management Protocol/Oakley," abbreviated as ISAKMP/Oakley. This protocol allows the receiver to obtain a public key and identify ("authenticate") the sender via digital certificates. This protocol also sometimes referred to more simply as "Internet Key Exchange" or IKE. IKE provides the keys for the IPSec protocols, and Security Associations (SA) are created based on the keys. A maximum of two decryption SAs are supported at a time in standard IPSec implementation.

[0010] Standard implementation of IPSec imposes inherent limitations on how frequently the keys can be changed. This is a central problem when attempting combine QKD and IPSec to increase security. As mentioned above, QKD is capable of providing many keys per second (e.g., 100 keys/second or even more), while IPSec's fastest key change rate is around once per second. To make use of the QKD-generated keys for IPSec, one would want to be able change them as fast as possible.

[0011] Also, IKE is used to provide keys for IPSec, and QKD is not a part of IKE. Accordingly, there is presently no way to incorporate QKD-generated keys into the IKE process so that QKD-generated keys can be used in IPSec.

SUMMARY OF THE INVENTION

[0012] The present invention relates to quantum cryptography and Internet communication, in particular relates to methods of integrating quantum key distribution (QKD) with Internet protocol security ("IPSec") to provide for enhanced security of Internet-based data communication.

[0013] Standard IPSec protocols impose limits on the frequency at which keys can be changed, making efforts to improve the security of IPSec by employing quantum keys

problematic. The method includes increasing the size of the Security Association (SA) Table in a manner that enables fast key flipping so that the quantum keys can be combined with the classical keys generated by Internet Key Exchange (IKE). The invention includes a method of creating the SA Table by combining (e.g., XOR-ing) quantum keys generated by the QKD process with classical keys generated by the IKE process, thereby enabling QKD-based IPSec.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] **FIG. 1** is a schematic diagram of the SA Table structure of the present invention adapted for fast key flipping, illustrating an exemplary implementation for three IPSec tunnels;

[0015] **FIG. 2** is a schematic diagram of the SA Table structure of **FIG. 1** for the transmitter side;

[0016] **FIG. 3** is a schematic diagram of the SA Table structure of **FIG. 1** for the receiver side; and

[0017] **FIG. 4** is a schematic diagram illustrating the steps of creating an SA that integrates QKD with IKE in parallel.

DETAILED DESCRIPTION OF THE INVENTION

[0018] As mentioned above, in the standard implementation of IPSec, each IPSec tunnel maintains two SA Tables, one for inbound data traffic and the other for outbound data traffic. Each Table, in turn, contains maximum of two SAs at a time. This imposes restrictions on how often the keys can be changed because IP packets might be delivered to decrypting side with delay and out of order. This happens especially often if the packets have to traverse Internet.

[0019] During transmission of information over the Internet, the IP packets can be delayed and can come out on the receiver side out of order. Thus, the SA needs to be long enough to ensure that all the encrypted packets are received in the proper order at the receiver and are properly decrypted.

[0020] Accordingly, an aspect of the invention involves increasing the SA Table size. This enables fast key flipping while also ensuring that the proper encryption/decryption and deliver order of the packets. Described below is an exemplary implementation based on the processor known under the trademark NITROX II, available from Cavium Networks, Santa Clara, Calif. The number of tunnels and SAs in a Table can vary for different implementations.

[0021] **FIG. 1** is a schematic diagram of the SA Table structure illustrating an exemplary implementation for 3 IPSec tunnels. **FIG. 1** illustrates a Cavium NITROX II (N2) memory that contain six SA Tables. Each IPsec tunnel uses two SA Tables, one for each direction of the traffic. Each SA Table contains up to 2^{16} SAs (32 Mbytes, or 0×2000000). "Flipping key" means using the next SA in the out-bound SA Table. There are up to three tunnels per N2 card: a data tunnel **0**: SA Table **0** (in- and out-bound), a data tunnel **1**: SA Table **1** (in- and out-bound), and a control tunnel: SA Table **2** (in-and out-bound). In operation, the host software sets up the SA Tables in N2 memory, and the N2 microcode accesses the SA Tables to encrypt/decrypt the packets.

[0022] **FIG. 2** is a schematic diagram of the SA Table structure on the transmitter side. There are 2^{16} SAs in each SA Table. Each SA is, for example, 512 bytes long. The SA Tables are numbered from 0 to 0×ffff.

[0023] Two SA pointers are used to manage the SA Table:

[0024] Active SA: SA number of currently active SA. The N2 microcode uses the SA pointed by Active to encrypt the packet. Initial value is 0.

[0025] Free SA: SA number of the first free SA slot. Appending a new SA increments Free SA by one wrapping around to 0 after $2^{16}-1$. Initial value is 0 indicating SA **0**.

[0026] The SA Table ID and the SA number in the SA Table are encoded in the security payload index (SPI) field of the ESP header. The decryption node extracts the SA Table ID and the SA number from the SPI field of the received packet to decrypt the packet. The encryption node advances the active SA to the next one when the time- or byte-lifetime expires.

[0027] **FIG. 3** is a schematic diagram of the SA Table structure on the receiver side. The receiver side structure is exactly the same structure as that of the transmitting side (**FIG. 2**). The receiver side extracts the SA Table ID and the SA number from the SPI field of the received packet and finds an appropriate SA. A large number of SAs in the memory ensures that SAs are not being removed from the memory before all reasonably delayed packets are decrypted. The key flipping rate and Table size determine the maximum allowable packet delay time. This delay can be adjusted by forming an appropriately sized SA Table.

Integrating QKD with IKE

[0028] As mentioned above, IKE provides "classic cryptography" keys for implementing standard IPSec. In general, QKD could directly replace IKE and "quantum keys" can be used instead of keys provided by IKE. A better approach however, is to combine QKD and IKE. This is a layered security approach because an attacker would need to break both layers to have an access to encrypted information.

[0029] **FIG. 4** is a schematic diagram illustration SA creation that integrates QKD with IKE. The SAs are created in three steps. First, a classic SA pair (in-bound and out-bound) are created using the standard IKE protocol. Second, a final SA pair is created from the classic SA pair by combining (e.g., XOR-ing) the encryption and authentication keys with the keys created by the QKD protocol. This process is carried out N times using different QKD keys. Third, the final N SA pairs are appended to the SA Tables automatically. A new classic SA pair may be created periodically according to standard IKE procedures.

[0030] As illustrated in **FIG. 4**, IKE and QKD are run in parallel. The final key used to create SA is a combination of the keys provided by IKE and QKD. In an example embodiment, the final key is an XOR value of the IKE and QKD keys (i.e., (classic key) XOR (quantum key)). In this approach, QKD lays transparently on top of the traditional cryptography. Accordingly, cracking the final key requires cracking both traditional and quantum cryptography. The entropy of the final keys is guaranteed to be equal to or greater than the entropy of the classical keys.

[0031] The creation of the final SAs from the classical SA takes very little time since it is a local operation. The SA

life-time can therefore be orders of magnitude shorter than the classical IKE re-keying time.

[0032] While the present invention has been described in connection with preferred embodiments, it will be understood that it is not so limited. On the contrary, it is intended to cover all alternatives, modifications and equivalents as may be included within the spirit and scope of the invention as defined in the appended claims.

What is claimed is:

1. A method of integrating quantum keys and classical keys for IPSec using Security Association (SA) Tables, comprising:

a) for each IPSec tunnel, creating an in-bound and out-bound classic SA pair using a standard Internet Key Exchange (IKE) protocol;

b) creating a final SA pair from the classic SA pair by combining classic keys associated with the classic SA pair with quantum keys;

c) repeating b) N times using different quantum keys to generate N final SA pairs; and

d) appending the final N SA pairs to corresponding inbound and outbound SA Tables.

2. The method of claim 1, wherein said combining includes XOR-ing the classic keys and the quantum keys.

3. The method of claim 1, including creating the classic keys and the quantum keys in parallel.

4. The method of claim 1, wherein the classic keys each include an authentication key and an encryption key.

5. A combined classical-quantum encryption method, comprising:

generating quantum keys via quantum key distribution;

providing classical keys via a Internet Key Exchange (IKE) protocol;

integrating the quantum keys and the classical keys to form combined quantum-classical encryption keys; and

performing IPSec with the combined quantum-classical encryption keys.

6. The method of claim 5, wherein each bidirectional IPSec communication includes a pair of Security Association Tables each having multiple security associations (SA) formed in a manner that enables fast key flipping.

7. The method of claim 6, including for each IPSec tunnel:

a) creating a classic SA pair (in-bound and out-bound) using standard IKE;

b) creating a final SA pair from the classic SA pair by combining encryption and authentication keys with the quantum keys; and

c) repeating step b) multiple times, each time using a different quantum key; and

d) appending the results of step c) to corresponding in-bound and out-bound SA Tables.

8. A method of performing an IPSec protocol, comprising:

generating quantum keys via quantum key distribution (QKD);

providing classical keys via Internet key exchange (IKE);

wherein the IPSec protocol employs a plurality of Security Association (SA) Tables of a standard size associated with a standard IPSec protocol, and including increasing the size of the SA Tables in a manner that enables a fast key flipping rate;

integrating the quantum keys and the classical keys to form combined quantum-classical encryption keys; and

performing the IPSec protocol with the combined quantum-classical encryption keys.

9. The method of claim 8, wherein the key flipping rate and an SA Table size determines a maximum allowable packet delay time, and including adjusting the packet delay time by adjusting the size of the SA Tables.

10. The method of claim 8, wherein the classical and quantum keys are integrated using an XOR-ing operation.

* * * * *